BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 31 No. 3. 2026

UDC 004.052.2:519.17
DOI: 10.62660/bcstu/3.2026.141

Method for integral assessment of incident criticality using causal graphs of service dependencies

Daniil Pylypenko*
Postgraduate Student
Lutsk National Technical University
43018, 75 Lvivska Str., Lutsk, Ukraine
https://orcid.org/0009-0004-4404-4715

Abstract. The relevance of the study is explained by the need to improve the accuracy of response prioritisation as digital infrastructures become more complex, since component interdependence and cascading propagation of failures can substantially increase the scale of adverse consequences. The study aimed to develop an approach for justified ranking of incidents by criticality, taking account of service interdependence and the scale of potential consequences. The methodological basis comprised system analysis, abstraction, formalisation, graph modelling, and conceptual modelling, which were used to examine service dependencies and substantiate an approach to assessing incident criticality in complex information systems. The study established that traditional approaches to incident criticality assessment are locally oriented and do not account for inter-service dependencies, cascading effects, or the architectural context of modern service-oriented information systems. As a result, systemic consequences can be underestimated. Incident criticality was substantiated as an integral characteristic that depends not only on the direct technical impact, but also on the structural importance of the affected service and the way impact propagates through the dependency network. The combination of these factors provided a more accurate representation of the actual level of systemic risk. A graph model of service infrastructure and a conceptual approach to integral criticality assessment were proposed, combining technical, structural, cascading, and business indicators through multilevel aggregation. Accounting for cascading effects and the structural importance of services was necessary for accurate incident assessment, as it allowed both direct and indirect consequences to be considered and the potential for local failures to develop into systemic disruptions to be determined. The results can be used by cybersecurity specialists, information-system architects, and analysts at incident monitoring centres in public and corporate IT infrastructures to improve the accuracy of incident prioritisation and systemic risk assessme

Keywords: odigital infrastructure; service-oriented architecture; cascading effects; multi-criteria analysis; information systems; risk analysis

INTRODUCTION

The relevance of the study arose from the increasing complexity of digital infrastructures, in which the operation of individual services depends on numerous interdependencies. Under these conditions, even local disruptions can produce large adverse consequences through cascading propagation of impact between system components. Traditional approaches to incident assessment mainly examine the direct consequences of events and give insufficient attention to the architectural features of the service environment. This makes response prioritisation less reliable and can lead to underestimation of systemic risks. Approaches are therefore needed that account for the structure of relationships between components of the digital ecosystem

Article's History: Received: 13.04.2026; Revised: 07.08.2026; Accepted: 21.09.2026; Published: 07.10.2026

Suggested Citation:
Pylypenko, D. (2026). Method for integral assessment of incident criticalityusing causal graphs of service dependencies. *Bulletin of Cherkasy State Technological University*, 31(3), 141-157. doi: 10.62660/bcstu/3.2026.141.

*Corresponding author (daniilpylypenko@hotmail.com)

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

and for possible mechanisms through which adverse impact may propagate when decisions on incident response are made.

In Ukrainian scientific society, incident criticality assessment and analysis of interdependencies between information-system components are increasingly considered through system analysis, graph modelling, and intelligent data processing. V.I. Pevnev (2026) examined approaches to optimising integrated video-surveillance systems using data-analysis methods to improve monitoring and decision support. The reported results supported the use of analytical models for prioritising events in complex information environments, but criticality assessment based on service dependencies was outside the scope of that study. T. Savchenko *et al.* (2025) proposed a systematic approach to cyber-threat analysis based on risk models and graph structures for examining cyberattack and penetration-testing processes. The authors reported that a graph representation of relationships between network-infrastructure objects made it possible to trace attack scenarios, identify the most vulnerable nodes, and assess the potential consequences of realised threats. Their conclusions supported the use of graph models for analysing complex systemic interdependencies, providing a basis for further development of methods for integral assessment of incident criticality. M. Karpinsky *et al.* (2015) developed a method for detecting incidents and potential crisis situations in information systems. The approach was intended to identify hazardous events promptly by analysing a set of indicators and assessing their level of danger. The study underlined the value of formalising incident-assessment processes for more effective response, but concentrated on event detection rather than on determining criticality by accounting for causal dependencies between services.

Other publications gave increasing attention to automation of incident-management processes and to intelligent mechanisms for assigning priority. L. Annadata (2023) proposed an approach to incident handling in a DevOps environment based on data from previous events, their characteristics, and response outcomes. Historical data on earlier incidents, including failure types, frequency, resolution time, affected components, and consequences for services, were used to determine criticality more accurately, improve event classification, and reduce response time through automated prioritisation and better allocation of resources among support teams. N. Chandu (2025) analysed the use of artificial intelligence to improve incident detection, classification, and resolution. The author argued that machine-learning algorithms can rapidly determine the importance of events, automate their categorisation, and support decisions during response. The results supported the potential of intelligent approaches for faster incident management. However, event criticality was still assessed mainly from the characteristics of each event, without accounting for cascading impact on related services and business processes.

A. Peralta *et al.* (2025) further reinforced incident-prioritisation methods by proposing a hybrid mathematical model for dynamic priority assignment based on fuzzy Q-learning and analysis of textual incident descriptions. The approach combined adaptive-learning mechanisms with processing of unstructured data, allowing the priority level to be adjusted automatically according to context and accumulated experience. Experimental testing produced more accurate incident rankings than traditional methods. J. Beyza *et al.* (2020), in turn, examined the criticality of interdependent power and gas-transmission systems using complex-network methods and flow-distribution analysis. Their modelling established that failures of individual nodes can propagate to connected subsystems, creating cascading effects and substantially increasing potential losses. These results supported accounting for inter-system dependencies when assessing the criticality of objects, since local disruptions can have much wider consequences across the infrastructure. S. Das *et al.* (2024) developed a related approach and proposed a graph-learning method for failure-criticality analysis to improve the functional safety of electronic and electrical systems. The authors used graph neural-network algorithms to identify components whose failure has the greatest effect on overall system operability. Their experiments found that a graph representation of dependencies between elements identified critical failure points more accurately than traditional approaches and could also predict possible consequences of fault propagation in complex technical environments.

The review of previous research established that most existing approaches focused either on the characteristics of individual incidents or on identifying critical nodes in technical and infrastructure networks. Integral assessment of incident criticality in information systems remained insufficiently examined when causal dependencies between services were considered, even though the impact of an incident can depend both on its local characteristics and on the potential for consequences to propagate through a network of interconnected components. General methodological approaches combining service-dependency analysis with quantitative assessment of incident criticality in one model were also lacking. The study therefore aimed to improve the justification of response prioritisation in complex information systems by accounting for relationships between services and the potential propagation of consequences. Two tasks were set: to analyse existing approaches to incident criticality assessment, service-dependency modelling, and response prioritisation in order to identify their advantages, limitations, and unresolved aspects; and to form a system of criteria for integral assessment of incident criticality based on causal relationships between services and substantiate

a mechanism for determining criticality with regard to the potential propagation of consequences through an interdependent service infrastructure.

MATERIALS AND METHODS

The study was theoretical-methodological and focused on developing a formalised approach to incident criticality assessment in complex service-oriented information systems. The methodology combined system analysis, theoretical and conceptual generalisation, and graph modelling as complementary procedures. The overall logic of the work centred on constructing a conceptual model for integral assessment of incident criticality by formalising causal dependencies between services, defining an assessment-criteria system, developing a mechanism for incorporating cascading effects, and substantiating an integral indicator capable of representing the systemic impact of incidents in multilevel digital infrastructures.

The materials of the study included generalised models of service-oriented information systems, typical scenarios of incident occurrence and development, structural schemes of inter-service dependencies, conceptual models of incident management, and modelled causal graphs of service relationships. The assessment criteria were formed from analysis of research publications, regulatory and methodological approaches to incident management, and current practices for criticality assessment in complex digital infrastructures. Causal graphs were constructed from typical service-dependency structures. This made it possible to examine potential paths of incident-impact propagation and mechanisms by which cascading effects arise in multilevel information systems.

The study used a set of interrelated theoretical methods, each with a separate functional role in developing the approach to incident criticality assessment. System analysis was used to treat the service-oriented information system as a complex multilevel structure in which individual components are connected by functional and technological dependencies. It supported decomposition of the service environment, identification of key infrastructure elements, examination of relationships between services, and justification for considering possible systemic consequences in addition to local incident characteristics. Abstraction was then applied to separate the most relevant characteristics of incidents and service dependencies from the particular implementation of an information system. This method defined general factors affecting incident criticality, including the degree of service degradation, duration of impact, structural importance of a component, potential for cascading propagation, and consequences for business processes. These factors provided a general basis for subsequent quantitative assessment. Formalisation converted the general characteristics into a system of parameters, criteria, and calculation rules. The procedures for indicator normalisation, principles for forming group indices, and rules for combining individual characteristics into an integral criticality assessment were defined at this stage. Qualitative properties of incidents were thereby represented as formalised variables suitable for mathematical analysis. Graph modelling was used to represent the structure of service dependencies, with the information system expressed as a directed weighted graph. Nodes represented individual services or components, edges represented dependencies between them, and edge weights characterised the strength of functional influence. The graph model was used to identify critical nodes, analyse direct and indirect dependencies, assess paths of impact propagation, and account for possible cascading effects. Multi-criteria analysis was used for quantitative determination of criticality, combining technical, structural, cascading, and business characteristics of incidents in one integral indicator. Normalised parameters were aggregated, partial indices were calculated, and the final criticality assessment was formed with weights for the separate criterion groups. Conceptual modelling was applied at the final stage to integrate the outputs of the methods into a single incident-criticality model that combined description of the service infrastructure, dependency analysis, assessment of cascading consequences, and decision support.

In the study, a cascading effect was defined as propagation of the adverse impact of an incident from the initially affected service to other system components through the network of service dependencies. Direct impact referred to effects on services that depended immediately on the affected node and were connected to it by one graph edge. Indirect impact covered services at the second and subsequent dependency levels, to which the adverse effect was transmitted through one or more intermediate nodes. An attenuation coefficient α, ranging from 0 to 1, was used to represent the reduction in impact strength as distance from the incident source increased. Impact on a node at dependency level k was calculated as the initial impact strength multiplied by α^k, representing the gradual decrease in the intensity of cascading propagation. Propagation stopped when the impact fell below threshold β or when subsequent nodes had no outgoing dependencies. Each node was counted only once when several routes led to the same service, which prevented double counting. Where several propagation paths reached a node, the maximum resulting impact value was used in the calculation. This procedure gave a consistent estimate of the scale of cascading incident propagation and prevented artificial inflation of the integral criticality indicator.

The graph model was used to analyse routes of incident-impact propagation, identify direct and indirect dependencies between services, and assess potential cascading effects. Graph characteristics included the number of dependent services, node reachability,

centrality of a node within the dependency network, depth of impact propagation, and lengths of routes along which adverse impact was transmitted. Cyclic links were treated as separate interdependency loops that could increase the risk of cascading consequences. Nodes with high centrality and a large number of dependent services were treated as critical because their failure could cause extensive disruption of the digital infrastructure. Graph modelling therefore formalised mechanisms of incident-impact propagation, assessed the structural importance of services, and substantiated inclusion of graph parameters in the integral criticality-assessment procedure.

An integral-assessment algorithm was applied to determine the criticality of individual service-infrastructure nodes, accounting for both local incident characteristics and potential impact on the connected service network. At the first stage, the information system was represented as a directed causal graph G = (V, E), where the node set V corresponded to individual services or system components and the edge set E represented directed dependencies between them. Structural and functional characteristics were determined for each node: the number of dependent services, degree of centrality, level of functional importance, and scale of possible disruption. The integral node-criticality indicator aggregated several assessment components: direct incident impact on the service, number of connected components, depth of consequence propagation, and importance of the service to operation of the system as a whole. Nodes with many dependent components and substantial influence on critical processes consequently received higher response priority. This moved the assessment from treatment of an incident as an isolated event to analysis of its systemic consequences. A cascading process was identified when disruption of one node caused a sequential decrease in availability or degradation of related components. Formally, a cascading effect was recorded when three conditions were met: an active connection existed between the affected node and a dependent service; the impact on the dependent component exceeded a critical threshold; and no automatic recovery or load-compensation mechanism was available. If the impact propagated through several dependency levels, the incident was classified as a multilevel cascade.

Qualitative incident characteristics included in the criteria system were converted into quantitative indicators through normalisation so that integral assessment could be performed. The parameters had different measurement properties, including temporal characteristics, degree of functional degradation, number of dependencies, and scale of user impact. All indicators were therefore converted to a common dimensionless scale from 0 to 1, where 0 represented no or minimal impact and 1 represented the maximum critical level. Four general assessment groups were formed: technical component T, structural component S, cascading component C, and business component B. Technical indicator T was determined from the level of service degradation, incident duration, recovery complexity, and potential security threat. Each parameter was assessed on a five-point scale, where 1 represented minor impact and 5 a critical disruption of service operation. The values were then normalised using equation (1):

$$X_n = \frac{X - X_{min}}{X_{max} - X_{min}}, \quad (1)$$

where X_n – the normalised indicator value, X – the obtained score, and X_{min} and X_{max} – the minimum and maximum values of the scale. Structural indicator S was formed based on the number of dependent services, node centrality, position in the service-dependency graph, and functional importance. The number of dependencies and node centrality were determined from the characteristics of the causal graph, after which the resulting values were also converted to a range from 0 to 1. Higher S values corresponded to services on which more system components depended. Cascading indicator C was determined by analysing possible propagation of incident impact. The calculation included the number of potentially affected nodes, propagation-path length, and strength of dependencies between components. C increased where disruption of one service could cause secondary failures at several infrastructure levels. Business indicator B described organisational consequences of an incident and included impact on key business processes, the number of users affected by loss of service availability, and the level of operational losses. Each criterion was assessed by experts on a scale from 1 to 5 and then normalised. Once all parameters had been converted to a common scale, the integral incident-criticality indicator was calculated as a weighted sum of the general components (2):

$$K = w_T T + w_S S + w_C C + w_B B, \quad (2)$$

where K – the integral level of incident criticality; w_T, w_S, w_C, and w_B – weighting coefficients for the corresponding criterion groups, with a sum of 1. The procedure converted qualitative descriptions of incident characteristics into a formal numerical assessment. This allowed different incidents to be compared, their priority to be determined, and both the local failure and potential systemic impact to be considered.

A classification scale was developed for practical interpretation of the integral criticality indicator. All local indicators had first been normalised to the interval from 0 to 1, and the integral indicator also took values within [0;1]. The value range was therefore divided uniformly for interpretation. The full interval [0;1] was split into five equal subintervals with a width of 0.20, each corresponding to a separate criticality level. This provided an unambiguous interpretation of the results,

simplified incident prioritisation, and allowed the same classification criteria to be used regardless of the characteristics of a particular information system. An incident was assigned to a criticality level according to the value of the integral indicator IC.

RESULTS

Theoretical basis for integral assessment of incident criticality

Traditional approaches to incident criticality assessment are based mainly on local event characteristics, such as the level of impact on an information asset, the number of users affected by disruption of a service, downtime, financial losses, or the extent to which information-security requirements are breached. Although these approaches are widely used in information technology (IT) service-management systems and security monitoring centres, their methodological basis largely treats an incident as an isolated event and gives insufficient consideration to structural interconnections between components of digital environments. Incident criticality is therefore determined mainly from the immediate consequences of occurrence, while indirect effects and cascading mechanisms of impact propagation remain insufficiently represented. Further analysis linked this limitation to the evolution of information systems from relatively autonomous software and hardware complexes to multilevel service-oriented architectures, where individual services form a complex dependency network. Under these conditions, operation of the final business process depends not only on the state of one service, but also on the reliability of the entire chain of interconnected components. Disruption of even a secondary service can consequently have disproportionately large effects when that service contributes to critical higher-level services. Traditional assessment methods that do not account for service-infrastructure topology have limited capacity to represent the actual scale of potential incident consequences (Leal *et al.*, 2024). Theoretical generalisation of existing approaches identified several fundamental limitations that complicate objective assessment of incident criticality in complex digital ecosystems (Table 1).

Table 1. Main limitations of traditional approaches to incident criticality assessment

Limitation	Nature of the problem	Potential consequences
Localised assessment	Only the characteristics of an individual incident are analysed	Underestimation of systemic consequences
Static criteria	Fixed impact indicators are used	Loss of adaptability to architectural changes
Service dependencies ignored	Relationships between services are not considered	Errors in priority determination
No cascading analysis	Indirect incident consequences are not assessed	Underestimation of criticality
Focus on individual assets	Analysis is performed at the resource level rather than the service level	Incomplete representation of business impact
Limited consideration of system structure	Architectural characteristics are not included in calculations	Low assessment accuracy

Source: compiled by the author based on S. Ghosh *et al.* (2024), T. Liu & F. Liu (2025)

Analysis of the general limitations revealed that traditional approaches to incident criticality assessment do not adequately represent the complexity of modern service-oriented systems because they focus mainly on local event characteristics. Systemic consequences arising from service interdependence and cascading impact propagation can therefore remain underestimated. A central limitation is that the structural organisation of the information infrastructure is not incorporated, which reduces the reliability of incident prioritisation. Insufficient attention to indirect effects can also produce an assessment below the actual criticality of events in complex digital ecosystems. The generalisation supported a shift towards models in which inter-service dependencies and cascading effects are treated as determining factors of criticality. These limitations arose from the absence of a mechanism for integrating structural information about the service infrastructure into the criticality-assessment procedure. In most existing models, an incident is treated as a source of direct impact on a particular service or resource, although the actual effect can spread much further through networks of functional, technological, and logical dependencies. From the perspective of complex-systems theory, this produces emergent effects in which the combined consequences of a disruption exceed the simple sum of local effects on individual components.

Thus, a transition from a resource-oriented to a service-oriented paradigm of incident criticality assessment was substantiated. The main feature of this approach was recognition that a service does not operate in isolation, but within a dependency network where its operability is determined by the state of other interconnected services. Incident criticality should consequently depend on both the characteristics of the incident and the position of the affected service within the overall structure of the digital ecosystem. Service dependencies were conceptualised as directed causal relationships between components of the information

infrastructure. Within this approach, each service can simultaneously consume functionality provided by other services and supply its own functions to higher-level services. This creates a multilevel structure of interdependencies in which disruption of one node can potentially trigger a chain of degradation across adjacent components (Fig. 1).

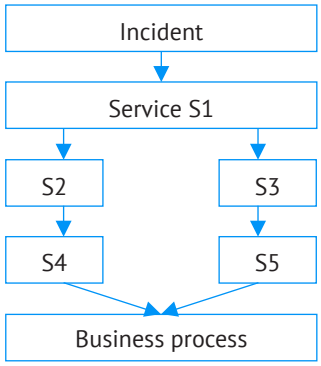


Figure 1. General model of incident-impact propagation through service dependencies
Source: compiled by the author based on P. Fang *et al.* (2022)

Analysis of the model established that incident impact extends beyond the directly affected service to related components at lower levels. As service dependencies branch, the initial disruption develops into a cascading effect that simultaneously covers several services and ultimately affects execution of the business process. Unlike traditional models, where assessment ends at service S1, the proposed approach examines the entire impact-propagation path through to final business processes. This mechanism accounts for both direct and indirect consequences of an incident, which is particularly relevant to modern distributed digital platforms.

The theoretical review also defined basic principles for an integral method of incident criticality assessment. The first was structural dependence: the criticality level is determined not only by incident properties, but also by the position of the affected service in the architecture of the information system. The second was cascading impact, which requires possible propagation of adverse consequences through the service-dependency network to be considered. The third was integral assessment, under which final criticality is formed by combining technical, functional, architectural, and business characteristics of an incident in one analytical indicator. The fourth principle was hierarchical analysis, allowing the multilevel structure of modern service ecosystems to be represented. Together, these principles provided a theoretical basis for moving from conventional local incident assessment to an integral approach centred on analysis of causal graphs of service dependencies (Raptaki *et al.*, 2024). This concept supports a more accurate determination of the actual incident-criticality level and further formalisation of mechanisms for incorporating cascading effects in complex digital infrastructures.

Formalisation of causal relationships between services and incidents

Effective assessment of incident criticality in digital environments requires a formal representation of the structure of interdependencies between services, because the nature of these relationships determines the scale of adverse impact propagation and the level of potential risk to operation of the information infrastructure. Traditional hierarchical models of information systems usually focus on organisational or functional decomposition of components and do not sufficiently represent the actual mechanisms through which dependencies are transmitted between services. The study therefore used a graph approach to formalise the service ecosystem as a set of interconnected objects and represent complex causal relationships between them.

The service infrastructure was represented as a directed graph , where set described the collection of services, components, and business functions, while set represented dependencies between them. A directed graph was used because most service relationships are asymmetric: operation of one service may depend on another without a reciprocal dependency. This structure made it possible to trace directions of incident-impact propagation and identify critical nodes through which many service interactions pass. In the proposed model, each graph node represented a separate element of the service infrastructure involved in creating, transmitting, or processing information. The graph was not limited to software services and covered all levels of the digital ecosystem, including hardware resources, network infrastructure, application services, and business processes. This provided a coherent representation of the operating environment of the information system and allowed incident effects to be considered at different architectural levels. Nodes were classified by functional purpose to improve analytical accuracy (Table 2).

Table 2. Typology of nodes in the causal graph of service dependencies

Node type	Notation	Characteristic
Infrastructure node	N_I	Servers, network devices, data storage systems, and virtualisation platforms
System service	N_S	Databases, authentication services, and middleware components
Application service	N_A	Business applications, web services, and API components

Continued Table 2.

Node type	Notation	Characteristic
Business service	N_B	Services directly related to implementation of business functions
Business process	N_P	Final organisational processes that create business value

Notes: five main components were considered for integral assessment of incident criticality: incident-impact intensity (N_I), criticality of service dependencies (N_S), number of affected nodes (N_A), scale of consequence propagation (N_B), and cascading-propagation potential (N_P). Considering these parameters together allowed both local incident consequences and systemic impact on operation of the information infrastructure to be assessed. API – Application Programming Interface
Source: compiled by the author based on M. Ghalenoei *et al.* (2024), P. Chakraborty *et al.* (2025)

Analysis of the proposed typology established that the causal-graph structure covered all principal levels of the digital ecosystem, from basic infrastructure to business processes. This gave a coherent representation of the service environment and allowed local technical disruptions to be traced as they developed into consequences for organisational business functions. Separating the node types helped organise service dependencies and provided a basis for analysing routes of impact propagation between architectural levels. The graph model could therefore be used both to describe the structure of an information system and to examine mechanisms of cascading effects and identify potentially critical elements of the service infrastructure.

In addition to formalising nodes, the study defined a system of links describing the nature of interactions between components. Analysis of service-oriented architectures established that dependencies can differ in nature, impact strength, and degree of criticality. Several link types were therefore proposed to represent the actual structure of the information system more adequately (Table 3).

Table 3. Classification of links in the causal graph

Link type	Notation	Characteristic
Functional dependency	E_F	One service uses functions of another service
Information dependency	E_D	Data transfer or shared use of data
Technological dependency	E_T	Shared use of infrastructure resources
Logical dependency	E_L	Relationship between components at the business-logic level
Process dependency	E_P	Participation of a service in execution of a business process

Source: compiled by the author based on S. Rötzer *et al.* (2022)

From a graph-theory perspective, each link was characterised by direction and weight. Direction defined the sequence of impact propagation, while weight represented the degree of dependency between components. High weight values corresponded to critical dependencies whose disruption could produce extensive consequences for many services. The mechanism of incident-impact propagation was formalised from the resulting graph structure. An incident arising at one node was not limited to a local effect; it initiated transfer of adverse impact through the dependency system. The intensity of propagation was determined by graph topology, the number of alternative interaction routes, and the strength of links between nodes.

The analysis established that the intensity of cascading propagation depended strongly on the structural position of a node in the dependency network. Central nodes through which many interactions routes pass had greater potential to generate systemic risk. Peripheral nodes, by contrast, generally produced local consequences that did not extend to other infrastructure components. An impact trajectory was introduced to describe propagation and was defined as an ordered chain of nodes and links through which incident consequences are transmitted. Multiple trajectories between the incident source and final business processes represented a higher level of systemic importance for the corresponding node. In such cases, even a minor local failure could develop into a large disruption of the digital ecosystem. On this basis, the causal graph was treated not only as a means of visualising service dependencies, but as a formal analytical model capable of representing the structure of relationships between information-infrastructure components, identifying potential routes of adverse-impact propagation, and providing a basis for subsequent integral assessment of incident criticality (Krupalija *et al.*, 2022). Including structural graph characteristics in the assessment procedure made it possible to move from analysis of individual events to examination of their systemic consequences, which is required when determining incident criticality in modern service-oriented information systems.

Conceptual model for integral assessment of incident criticality

Theoretical generalisation of existing incident-analysis approaches and formalisation of causal dependencies between services provided the basis for constructing a conceptual model of integral incident criticality assessment. Such a model was needed because most current criticality-assessment methods analyse individual incident characteristics in isolation and do not sufficiently

account for structural features of the service infrastructure. Criticality is consequently determined mainly from local event parameters, while architectural context, service dependencies, and cascading effects are insufficiently represented in the decision process.

The conceptual model was treated as a formal system of interconnected components intended to integrate heterogeneous incident characteristics in one assessment mechanism. Its main idea was to combine traditional indicators of impact and response urgency with service-architecture parameters describing the structural position of affected components in the dependency network. This moved the analysis from local assessment of a single event to examination of potential consequences across the digital ecosystem. At the conceptual level, the model assumed that incident criticality was formed by three complementary groups of factors. The first comprised direct incident characteristics describing technical parameters and the scale of initial impact. The second described architectural features of the service infrastructure and the structural importance of affected components. The third covered cascading consequences as impact propagated through the service-dependency network. Integration of these factors allowed a more objective assessment of criticality in complex digital environments (Krupalija *et al.*, 2022). Figure 2 presents the general structure of the conceptual model.

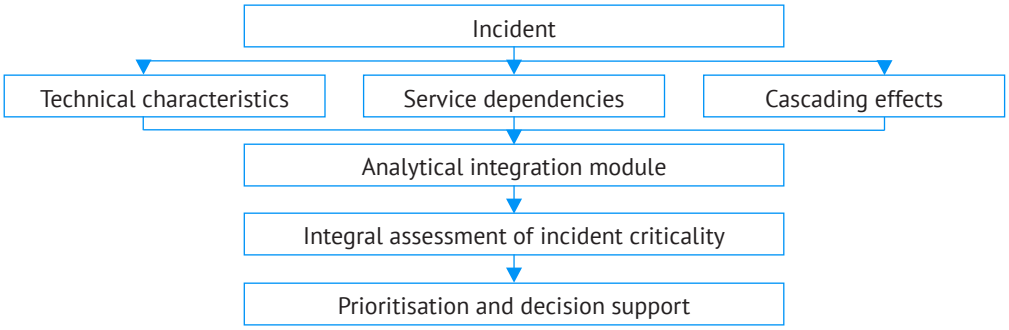


Figure 2. Structure of the conceptual model for integral assessment of incident criticality
Source: compiled by the author

Analysis of the functional structure of the model identified several interconnected components, each with a separate role in forming the integral assessment. The components were combined within an integration module that aggregated the resulting data. This element converted multiple local assessments into one integral criticality indicator. Conceptually, the integration module formed the analytical core of the assessment system because it combined information on incident characteristics, service-infrastructure topology, and the scale of cascading impact. A general description was prepared to clarify the functional purpose of each component (Table 4).

Table 4. Main components of the conceptual model

Model component	Functional purpose and role in the assessment process
Incident description module	Provides the initial representation of an incident by recording its type, source, time of occurrence, scale of initial impact, and characteristics of the affected service. The resulting parameters form input data for further analysis
Service-dependency analysis module	Constructs and analyses the graph of relationships between services. Identifies dependent components, structurally important nodes, and direct and mediated links that may affect propagation of incident consequences
Cascading-consequence assessment module	Analyses possible incident-development scenarios through the dependency network. Determines the depth of impact propagation, number of potentially affected components, and probability of secondary disruption of system operation
Integral criticality calculation module	Combines analysis of incident characteristics, service dependencies, and cascading effects into a single criticality indicator. Provides a quantitative comparison of incidents by their level of potential threat to the information system
Integration module	Coordinates the results of separate analytical blocks, aggregates indicators, and forms a general assessment of incident impact while accounting for systemic interdependencies
Decision-support module	Uses the criticality assessment to determine response priority, allocate resources, and select the first measures for mitigating incident consequences

Source: compiled by the author based on A. El-Maissi *et al.* (2024)

Analysis of the model structure established a sequential organisation from collection and processing of initial information to formation of final management conclusions. Each component performed a separate

analytical function while remaining integrated into the overall assessment process. The combined operation of the components linked analysis of incident characteristics, service-architecture features, and potential systemic consequences within one information flow. This arrangement supported determination of criticality and provided a basis for justified incident prioritisation.

Conceptual modelling established that the proposed approach depended substantially on interaction between the individual system components. Unlike linear assessment models, where information flows sequentially from one stage to another, the proposed structure provided continuous information exchange between modules. Results of service-dependency analysis, for example, were used not only to assess cascading consequences, but also to refine the initial incident description by accounting for the structural importance of the affected service. The actual logic of the model was therefore not limited to sequential information transfer (Kosmowski *et al.*, 2022). Results of cascading-effect analysis could modify the structural importance assigned to individual services, while integral-assessment results could be used to revise parameters of dependency analysis. This formed a closed analytical loop in which each component performed its own functions and also helped maintain consistency across the assessment system. The conceptual model provided a theoretical basis for further formalisation of criteria and indicators of incident criticality. Unlike existing approaches, it integrated technical incident characteristics, structural parameters of the service infrastructure, and cascading mechanisms of impact propagation in one analytical construction, allowing criticality to be treated as a complex characteristic of the functional state of a digital ecosystem.

System of criteria and indicators for criticality assessment

Development of an integral method for incident criticality assessment required a criteria system capable of representing the multidimensional nature of incident impact in modern service-oriented information systems. Theoretical analysis established that one indicator could not provide sufficient coverage because incident criticality is formed by technical, architectural, functional, and organisational factors. A multi-criteria approach was therefore proposed in which the final assessment integrates several groups of indicators representing different aspects of incident impact on operation of the digital ecosystem. This was necessary because incidents with the same local characteristics can differ substantially in systemic consequences depending on the position of affected services in the dependency structure (Reyes-Acosta *et al.*, 2025). A short disruption of a central authentication service, for example, can produce much greater losses than a prolonged failure of a peripheral component even when both incidents have the same duration and technical parameters. The criteria system therefore had to account for both direct incident characteristics and potential impact on the architecture of the service infrastructure. Four complementary criterion groups were formed: technical criteria, structural criteria, cascading-impact criteria, and business-oriented criteria. This division covered the factors determining the actual incident-criticality level. Table 5 presents the resulting criteria system.

Table 5. Criteria system for integral assessment of incident criticality

Criterion group	Local indicator	Indicator content
Technical	Level of service degradation	Degree of functional disruption
	Incident duration	Duration of adverse impact
	Recovery complexity	Resources required to mitigate consequences
	Security-threat level	Potential breach of confidentiality, integrity, and availability
Structural	Number of dependent services	Scale of architectural impact
	Node centrality	Importance of the service within the dependency network
	Position depth	Position of the service in the architectural hierarchy
	Service criticality	Role of the service in maintaining system operation
Cascading	Number of potentially affected nodes	Scale of impact propagation
	Length of propagation paths	Potential for cascading effects
	Intensity of impact transmission	Strength of dependencies between services
Business	Impact on business processes	Disruption of core activities
	Impact on users	Scale of reduction in service quality
	Level of operational losses	Consequences for current processes

Source: compiled by the author based on D. Samia & F. Innal (2023), C. Wen (2024), L. Zhu *et al.* (2025), C. Zheng *et al.* (2026)

As Table 5 shows, each indicator represents one aspect of criticality and cannot by itself provide an adequate assessment of incident complexity. Duration, for example, describes the temporal aspect of impact but does not account for the architectural importance of a service. Node centrality represents structural role, but

does not measure the actual scale of functional disruption. Local indicators therefore had to be integrated within one analytical mechanism. The criteria system also corresponds to the multilevel structure of service infrastructure. Technical indicators describe the local operating level of an individual service. Structural criteria represent the architectural level of relationships between services. Cascading indicators describe inter-level propagation of impact, while business criteria represent final consequences for organisational activity. The incident can thus be followed from its occurrence through to effects on final business processes. The resulting criteria system provided the theoretical basis for assessment of incident criticality in service-oriented information systems. In contrast to traditional models that focus mainly on local event characteristics, the proposed approach integrates technical, structural, cascading, and business aspects of impact in one analytical construction. This multidimensional set of indicators provided the basis for forming an integral criticality indicator and developing a formal procedure for its calculation.

Method for integral calculation of incident criticality accounting for service dependencies and cascading effects

After the criteria system and local indicators had been formed, the next stage was development of a method for integral calculation of incident criticality. The method was intended to combine heterogeneous incident characteristics in one analytical indicator. This mechanism was required because criticality is multidimensional and cannot be represented adequately by separate local indicators. The analysis established that an incident may simultaneously have high technical impact, low architectural importance, and moderate business consequences. Conversely, a small local impact may have substantial potential for cascading propagation through critical service dependencies. Decisions based on separate indicators are difficult under these conditions and can lead to subjective response priorities.

An integral approach was therefore proposed in which criticality was treated as an aggregated characteristic formed by several groups of factors. The integral indicator had to represent not only the scale of direct disruption of service operation, but also the architectural importance of the affected component, potential propagation of adverse impact through the dependency network, and final consequences for organisational business processes (Zheng *et al.*, 2026). The method was based on multi-criteria integration, with the general criticality level determined through stepwise aggregation of local assessments. Indicators with different properties could therefore be considered simultaneously without losing information about their contribution to the final assessment. Figure 3 presents the general structure of the integral indicator.

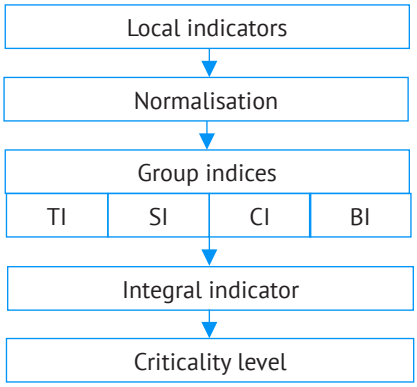


Figure 3. Formation of the integral criticality indicator

Notes: in the proposed method, the integral assessment of incident criticality is formed from four interrelated components: technical impact index TI, structural impact index SI, cascading impact index CI, and business impact index BI

Source: compiled by the author based on B. Coutinho *et al.* (2023)

Analysis of the scheme established that the proposed approach used a hierarchical assessment principle in which heterogeneous incident characteristics were progressively converted into one general result. This organisation combined different aspects of event impact in a single analytical model while retaining their substantive differences. The final assessment was based on joint consideration of technical, architectural, cascading, and business factors. This allowed criticality to be determined more objectively than with approaches based on only individual indicator groups. A general weighted-aggregation model was used for formal description of the integral assessment (equation 2). The proposed model also allowed the assessment procedure to be adapted to a particular information system by changing the weights of individual components. In critical infrastructure, for example, the weights of business and cascading factors can be increased, whereas local technical systems may place greater weight on technical incident characteristics.

Directly combining all local indicators in one formula was found to remove the structural logic of the assessment. The proposed method therefore used a multilevel aggregation mechanism. At the first level, local indicators were integrated within each criterion group. The technical index, for example, was formed by aggregating service degradation, incident duration, recovery complexity, and security-threat level. Structural, cascading, and business indices were calculated in the same way. At the second level, the group indices were combined into the final integral assessment. This retained interpretability and allowed the contribution of each criterion group to the general criticality level to be examined. Figure 4 presents the logic of multilevel aggregation.

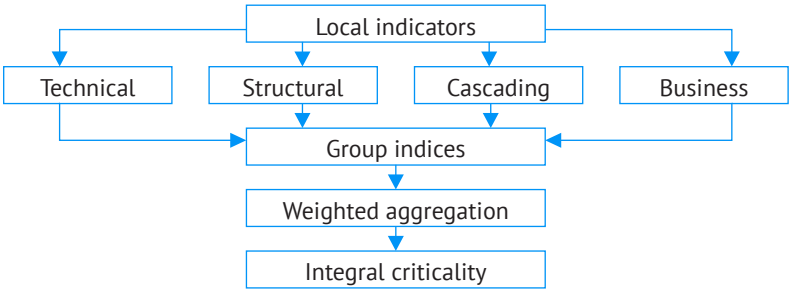


Figure 4. Multilevel aggregation procedure
Source: compiled by the author based on S. Gnatyuk *et al.* (2024)

A feature of the proposed approach was the inclusion of structural parameters from the service-dependency graph in the aggregation procedure. Traditional methods usually assess incident impact mainly from local event characteristics. The proposed model additionally accounted for topological features of the service infrastructure. This represented the systemic importance of the affected node and the scale of potential cascading propagation of adverse impact. The integral indicator was therefore formed from two complementary components: the actual impact of the incident and its potential systemic impact through the service-dependency structure. An interpretation scale was formed for practical use of the integral assessment. Its purpose was to convert numerical values of the integral indicator into categories suitable for management decisions on incident-response prioritisation. A five-level criticality system was proposed (Table 6).

Table 6. Interpretation of the integral criticality indicator

Value range	Criticality level	Characteristic
0-0.2	Very low	The incident is local and affects only an individual system component or function. The disruption does not cause a noticeable reduction in service availability, create a risk of propagation to other components, or affect business processes
0.21-0.4	Low	The incident has a limited impact on one or several services, but its consequences remain controllable. Interdependent system components largely remain operational, and the risk of cascading failures is minor
0.41-0.6	Medium	The incident has a noticeable effect on system operation and reduces service quality or causes partial loss of functionality. Consequences may propagate to connected components, requiring a prompt response
0.61-0.8	High	The incident affects several interdependent services and may disrupt key functions of the information system. There is an increased risk of cascading effects, substantial reduction in service availability, and adverse effects on users and business processes
0.81-1	Critical	The incident is systemic and involves critical infrastructure components. Consequences may propagate through the service-dependency network, causing cascading failures, substantial operational losses, disruption of business processes, and a need for immediate response

Source: compiled by the author

The proposed scale provided a unified interpretation of results regardless of the characteristics of individual services or architectural features of the information system. Boundaries between levels may nevertheless be adjusted to a particular domain, organisational requirements, or regulatory documents on risk and incident management. The formalised method used a multilevel procedure to aggregate local indicators structured according to the conceptual assessment model. Unlike traditional approaches, it accounted for direct incident characteristics, architectural features of the service infrastructure, and the potential for cascading propagation of adverse impact. The integral indicator therefore acted as a complex measure of systemic criticality and supported more justified incident prioritisation in complex digital environments.

Mechanism for accounting for cascading effects in the service-dependency graph

Service-oriented information systems are characterised by a complex network of interdependencies between infrastructure components. In traditional monolithic systems, incident consequences are usually confined to the local environment in which the event occurs. In multilevel digital ecosystems, disruption of one service can instead cause sequential degradation of many other components. Theoretical analysis established those cascading mechanisms of impact propagation are one of the main reasons why the initial characteristics of an incident can differ from its actual consequences for the information system. The proposed method therefore included a mechanism for accounting for cascading effects, so that criticality assessment covered both direct incident consequences and the potential scale

of subsequent propagation through the service-dependency network. A local incident assessment often does not represent actual systemic importance. Failure of an auxiliary authentication service, for example, may initially affect only one infrastructure component, but a large number of dependent services can allow the consequences to spread across the digital platform. Under these conditions, criticality depends on both the scale of the initial disruption and the structure of the interdependency network through which adverse impact is transmitted (Li *et al.*, 2025).

Incident consequences were considered as a combination of direct and indirect impacts. Direct consequences arise in the affected service itself or in components connected to it directly in the dependency graph. Indirect impacts arise when disruption propagates through several levels of service relationships and may occur even in components that have no direct connection to the incident source. Propagation distance was used to formalise this mechanism. The distance represents the number of graph edges through which adverse impact passes from the incident source to a particular service. Direct impact therefore corresponds to a distance of one, while indirect impacts occur at distances of the second, third, and subsequent orders. Figure 5 summarises the direct and indirect impacts of an incident.

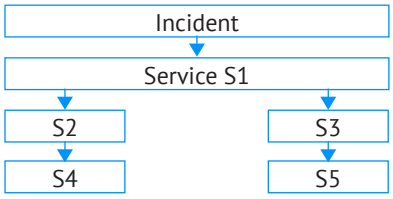


Figure 5. Direct and indirect impacts of an incident

Notes: S1-S5 are conventional designations for services (nodes) of the information system in the service-dependency graph. Node S1 corresponds to the service in which the incident occurs, while S2-S5 represent dependent services to which its impact may propagate. Arrows between nodes show the direction of impact transmission and possible routes by which cascading consequences may develop

Source: compiled by the author based on H. Nguyen *et al.* (2022)

In the example, impact on services S2 and S3 was treated as direct, while the consequences for S4 and S5 were second-order indirect impacts. Analysis of the graph structure established that, in real service ecosystems, indirect impacts often considerably outnumber directly affected components. Their inclusion in criticality assessment is therefore necessary. The scale of adverse consequences also depended on the architectural position of affected services rather than only on their number. Accumulated propagation effect was introduced to represent this factor and described the total incident impact on all components within the affected area. Conceptually, the accumulated effect was formed by summing the contribution of each service reached by the adverse impact. The contribution of a node depended on the strength of its link to the preceding component and its distance from the incident source. Impact was assumed to weaken gradually as the trajectory became longer, although it did not disappear completely because even distant components may participate in critical functions. The accumulated effect was described theoretically using the general model:

$$CE = \sum_{i=1}^{n} I_i \lambda^{d_i},$$

where CE – the accumulated incident-propagation effect; I_i – impact on the i-th service; d_i – distance from the incident source to the corresponding node; λ – impact-attenuation coefficient; and n – the number of services reached by propagation.

The proposed approach accounts for both the extent of service-infrastructure coverage and the gradual decrease in impact intensity as propagation routes become longer. The analysis established that secondary and tertiary consequences often form a substantial part of overall incident criticality, particularly in distributed service environments where one component may serve dozens or hundreds of dependent services at the same time.

The structural role of a service in the information-system architecture is another factor in criticality assessment. Incident consequences depended substantially on the graph node in which the event occurred. Disruption of a peripheral component is usually local, whereas an incident at a central node can cause extensive degradation of the entire system. The model therefore included structural importance of a service, describing its role in supporting interaction among other infrastructure components. Three main characteristics were used to determine structural importance: the number of incoming and outgoing dependencies; the position of the node in the service-interaction network; and participation of the service in critical business processes. These characteristics were used to form a general classification of services (Table 7).

Table 7. Levels of structural importance of services

Level	Service characteristic	Potential cascading impact
Low	Peripheral service with limited connections	Minimal
Moderate	Service with local dependencies	Limited
High	Central service within an individual segment	Substantial
Critical	Key node of the digital ecosystem	Maximum

Source: compiled by the author based on H. Nguyen *et al.* (2022)

Analysis of service structural-importance levels established that potential incident consequences depended strongly on the position of the affected component within the service-dependency architecture. Peripheral services with few links had minimal potential for impact propagation, so their failure was usually limited to local functional disruption. Services with local dependencies could affect individual functional segments, but the scale remained limited. Central services within separate segments acted as concentration points for interactions between components, and their failure could therefore disrupt several interdependent services simultaneously. The highest structural importance applied to key nodes of the digital ecosystem through which many service dependencies passed. Incidents in these components could initiate cascading adverse impact across different architectural levels and produce systemic failures.

The proposed mechanism for accounting for cascading effects therefore integrated three interrelated aspects into criticality assessment: direct incident consequences, the accumulated effect of propagation through the service-dependency network, and the structural importance of affected components. Traditional approaches are confined mainly to local event characteristics. The proposed model also accounts for systemic incident consequences and provides a stronger basis for determining actual criticality in complex service-oriented information systems.

DISCUSSION

Research on incident management and system criticality assessment has gradually moved from descriptive approaches towards formal graph-based and algorithmic models that account for component interdependencies, the dynamics of failure propagation, and the need to prioritise events in large distributed environments. A general comparison of Z. Chen *et al.* (2021), I. Šarūnienė *et al.* (2024) and K. Adamos *et al.* (2024) identified a common methodological basis for incident criticality assessment: analysis of structural dependencies between components of complex systems and use of graph models to formalise these relationships. In these studies, criticality was treated not as a local property of an individual element, but as a systemic property arising from inclusion of that element in a network of functional or state-dependent relationships. This was consistent with the present study, in which incident criticality was also interpreted as an integral characteristic formed through causal graphs of service dependencies. The reviewed studies likewise described an uneven distribution of criticality within a system, where individual nodes or services exert a disproportionately large influence on overall infrastructure operability. In I. Šarūnienė *et al.*, this appeared in assessment of the functional importance of elements; K. Adamos *et al.* used state-dependent relationships and their effect on resilience of cyber-physical systems; and Z. Chen *et al.* used graph aggregation of incidents and identification of relationships in large service environments. The present study represented a similar effect through an integral model that identified critical nodes while accounting for cascading impact propagation, which gave the phenomenon a broader interpretation. The studies also supported graph modelling as a general analytical tool for complex infrastructures. I. Šarūnienė *et al.* implemented the graph logic indirectly through structural dependency analysis, K. Adamos *et al.* used state dependency graph models, and Z. Chen *et al.* represented incidents explicitly as a graph for aggregation. This is compatible with the causal graph approach used here, which extends conventional models by formalising impact direction and propagation mechanisms. The comparison also identified an important difference. I. Šarūnienė *et al.*, K. Adamos *et al.*, and Z. Chen *et al.* mainly considered either static importance measures or structural dependencies without fully representing the dynamics of cascading effects. The present study instead used an integral approach in which incident criticality depended on both dependency topology and the potential for transitive propagation through the system. This moved the analysis from descriptive comparison towards a more formal assessment of systemic incident consequences.

A review of J. Chen *et al.* (2020), Z. Chen *et al.* (2020) and I. Ahmed & T. Sohrab (2023) identified another, complementary line of current research in which attention shifts from purely structural modelling towards a combination of empirical incident analysis, scenario-based threat assessment, and greater use of intelligent methods in incident management. Unlike approaches focused only on graph structure, these studies also considered behavioural characteristics of incidents, the context in which they arise, and possibilities for automated decision support. This provides a broader analytical setting than classical criticality models. J. Chen *et al.*, for example, used empirical analysis of large incident datasets from online service systems and identified a mismatch between incident frequency and actual criticality. Response processes were heavily loaded by low-priority events. This partly corresponded to the logic of the present study because it also supported differentiation of incidents by impact level. The main difference is that prioritisation in that work was based on attributes of the incidents themselves, whereas the present study determined criticality through structural causal dependencies between services, allowing the systemic effect of impact propagation to be represented. I. Ahmed & T. Sohrab (2023) examined vulnerability criticality by analysing possible attack-development scenarios, relationships between network nodes, and the probability of exploitation by attackers. Their results

supported graph models for identifying the highest-risk components of information infrastructure and improving cyber-risk management. This was consistent with the present use of graph representations of system relationships to identify critical points and improve cyber-threat assessment. The present study extended that approach by incorporating additional risk parameters and focusing on adaptive management of information-system security. Z. Chen *et al.*, in turn, proposed a conceptual model of intelligent incident management centred on integration of data analytics and machine-learning methods for decision support. Their work was partly consistent with the present conclusions concerning the need to move towards proactive incident management.

I. Sperstad *et al.* (2021) proposed a graph framework for analysing the vulnerability of critical event sequences in power systems. The authors reported that graph structures could identify critical failure-development trajectories and assess their effect on system stability. These results were partly consistent with the present study because they also supported graph representation of dependencies for analysis of critical scenarios. A. Schweikert *et al.* (2021) proposed a simplified method for identifying inter-system dependencies in critical-infrastructure networks. The authors found that even simplified modelling of interdependencies could improve assessment of mutual influence between services and infrastructure components. This also corresponded to the present conclusions on the role of inter-service dependency analysis in determining element criticality. The earlier work, however, used a mainly simplified procedure for identifying dependencies without detailed modelling of causal relationships or integral assessment of cascading effects, both of which were developed in the present study. X. Bin Wee *et al.* (2022) developed a simulation approach for assessing the criticality of urban rail and interdependent infrastructure networks. Their modelling of relationships between transport and associated infrastructure systems identified vulnerable nodes and assessed the consequences of their failure for overall system operability. These results partly supported the present conclusion that inter-system dependencies should be considered when determining criticality. S. Cui *et al.* (2025) proposed an agent-based approach to structured graph traversal for root cause analysis of incidents in cloud applications. The authors found that agent mechanisms could identify primary causes of incidents more effectively in complex distributed systems with multilevel dependencies. This was consistent with the present results because it also supported graph representation of systemic relationships for incident analysis.

The reviewed literature showed that current approaches to system criticality and vulnerability assessment are based mainly on graph representations of dependencies and analysis of component interaction. Some studies, however, were limited either to event sequences in physical systems or to simplified identification of inter-service dependencies without integrating cascading effects into a single assessment model. The present study addressed these limitations through causal graphs of service dependencies and an integral approach to incident criticality assessment. This made it possible to account for both structural system complexity and the dynamics of incident-impact propagation.

CONCLUSIONS

The theoretical study established that traditional approaches to incident criticality assessment were oriented mainly towards local event characteristics such as downtime, the level of impact on individual resources, and direct losses. This methodology did not fully account for the complex structural organisation of modern service-oriented information systems, so systemic and indirect incident consequences remained underestimated. The main limitations of existing approaches were the omission of inter-service dependencies, absence of cascading-effect analysis, static assessment criteria, and insufficient consideration of the architectural context of digital ecosystems. Incident criticality was found to depend not only on direct consequences, but also on the structural position of the affected service in the dependency network and on the way, impact propagates between system components. These findings substantiated a transition from a resource-oriented to a service-oriented approach in which criticality is treated as an integral characteristic of digital-infrastructure operation.

Formalising the service infrastructure as a directed weighted graph made it possible to describe causal relationships between infrastructure nodes, system services, application services, business services, and business processes as one analytical system. Incidents propagated through a network of directed dependencies, while propagation intensity depended on graph topology, link type, and link weight. Central nodes had a higher level of systemic risk, whereas peripheral components were usually associated with local consequences. Incident criticality was determined by three interrelated components: direct technical impact, structural importance of the affected service, and cascading propagation of adverse effects.

A conceptual model for integral assessment of incident criticality was proposed. It uses multilevel aggregation of local indicators into group indices and then forms a general integral indicator. The approach combines technical, structural, cascading, and business criteria in one analytical construction while retaining interpretability of the results. Cascading effects were found to be important because a substantial share of incident consequences develops at more distant levels of the service infrastructure. The study was limited

by the use of general assumptions about the structure of service dependencies and did not incorporate domain-specific features or empirical data from large production systems. Further research should validate the proposed approach using real infrastructure data and extend the model by integrating machine-learning methods for automatic estimation of service-dependency weights and cascading-impact parameters.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None

REFERENCES

[1] Adamos, K., Stergiopoulos, G., Karamousadakis, M., & Gritzalis, D. (2024). Enhancing attack resilience of cyber-physical systems through state dependency graph models. *International Journal of Information Security*, 23, 187-198. doi: 10.1007/s10207-023-00731-w.

[2] Ahmed, I., & Sohrab, T.B. (2023). AI-driven vulnerability prioritization for enterprise networks: A quantitative study using attack-graph models. *American Journal of Advanced Technology and Engineering Solutions*, 3(4), 129-166. doi: 10.63125/s6qn2t38.

[3] Annadata, L.A. (2023). *A data-driven approach for incident handling in DevOps*. Retrieved from https://www.diva-portal.org.

[4] Beyza, J., Ruiz-Paredes, H.F., Garcia-Paricio, E., & Yusta, J.M. (2020). Assessing the criticality of interdependent power and gas systems using complex networks and load flow techniques. *Physica A: Statistical Mechanics and its Applications*, 540, article number 123169. doi: 10.1016/j.physa.2019.123169.

[5] Bin Wee, X., Herrera, M., Hadjidemetriou, G.M., & Kumar Parlikad, A. (2022). Simulation and criticality assessment of urban rail and interdependent infrastructure networks. *Transportation Research Record: Journal of the Transportation Research Board*, 2677(1), 1181-1196. doi: 10.1177/03611981221103594.

[6] Chakraborty, P., Caulfield, T., & Pym, D. (2025). Causality and decision-making: A logical framework for systems and security modelling. *arXiv*. doi: 10.48550/arXiv.2508.01758.

[7] Chandu, N.K. (2025). Transforming incident management: Leveraging artificial intelligence for enhanced detection, classification, and resolution. *Journal of Computer Science and Technology Studies*, 7(5), 938-945. doi: 10.32996/jcsts.2025.7.5.108.

[8] Chen, J., *et al.* (2020). How incidental are the incidents? Characterizing and prioritizing incidents for large-scale online service systems. In *Proceedings of the 35th IEEE/ACM international conference on automated software engineering* (pp. 373-384). New York: Association for Computing Machinery. doi: 10.1145/3324884.3416624.

[9] Chen, Z., *et al.* (2020). Towards intelligent incident management: Why we need it and how we make it. In *Proceedings of the 28th ACM joint meeting on European software engineering conference and symposium on the foundations of software engineering* (pp. 1487-1497). New York: Association for Computing Machinery. doi: 10.1145/3368089.3417055.

[10] Chen, Z., Liu, J., Su, Y., Zhang, H., Wen, X., Ling, X., Yang, Y., & Lyu, M.R. (2021). Graph-based incident aggregation for large-scale online service systems. In *Proceedings of the 36th IEEE/ACM international conference on automated software engineering* (pp. 430-442). London: IEEE. doi: 10.1109/ASE51524.2021.9678746.

[11] Coutinho, B., Ferreira, J., Yevseyeva, I., & Basto-Fernandes, V. (2023). Integrated cybersecurity methodology and supporting tools for healthcare operational information systems. *Computers & Security*, 129, article number 103189. doi: 10.1016/j.cose.2023.103189.

[12] Cui, S., Krishna, R., Jha, S., & Iyer, R.K. (2025). PRAXIS: Integrating program analysis with observability for root-cause analysis. In *2026 56th Annual IEEE international conference on dependable systems and networks (DSN)* (pp. 52-66). Charlotte: IEEE. doi: 10.1109/DSN69566.2026.00021.

[13] Das, S., Kundu, S., Madhusoodhanan, P., Viswanathan Pillai, P., Parekhji, R., Raha, A., Banerjee, S., Natarajan, S., & Basu, K. (2024). Graph learning-based fault criticality analysis for enhancing functional safety of e/e systems. In *Proceedings of the 61st ACM/IEEE design automation conference* (pp. 1-6). New York: Association for Computing Machinery. doi: 10.1145/3649329.3656498.

[14] El-Maissi, A.M., Kassem, M.M., & Nazri, F.M. (2024). Resilient critical infrastructures: An innovative methodological perspective for critical infrastructure (CI) integrated assessment models by inducing digital technologies during multi-hazard incidents. *MethodsX*, 12, article number 102561. doi: 10.1016/j.mex.2024.102561.

[15] Fang, P., Gao, P., Liu, C., Ayday, E., Jee, K., Wang, T., Ye, Y., Liu, Z., & Xiao, X. (2022). Back-propagating system dependency impact for attack investigation. In *31st USENIX security symposium* (pp. 2461-2478). Boston: USENIX.

[16] Ghalenoei, M., Biglari, B., & Zarei, E. (2024). Accident and safety causation analysis in sociotechnical systems using AcciMap. In E. Zarei (Eds.), *Safety causation analysis in sociotechnical systems: Advanced models and techniques* (pp. 191-211). Cham: Springer. doi: 10.1007/978-3-031-62470-4_9.

[17] Ghosh, S., Grover, K., Wong, J., Bansal, C., Namineni, R., Verma, M., & Rajmohan, S. (2024). Dependency aware incident linking in large cloud systems. In *Companion proceedings of the ACM web conference 2024* (pp. 141-150). New York: Association for Computing Machinery. doi: 10.1145/3589335.3648311.
[18] Gnatyuk, S., Sydorenko, V., Polozhentsev, A., & Sokolov, V. (2024). Method for managing IT incidents in critical information infrastructure facilities. *Cybersecurity Providing in Information and Telecommunication Systems II 2024*, 3826, 326-333.
[19] Karpinsky, M., Korchenko, A., & Hizun, A. (2015). A method for identifying incidents/potential crisis situations. *Information Security*, 17(2), 175-181.
[20] Kosmowski, K.T., Piesik, E., Piesik, J., & Śliwiński, M. (2022). Integrated functional safety and cybersecurity evaluation in a framework for business continuity management. *Energies*, 15(10), article number 3610. doi: 10.3390/en15103610.
[21] Krupalija, E., Cogo, E., Bećirović, Š., Prazina, I., & Bešić, I. (2022). Cause-effect graphing technique: A survey of available approaches and algorithms. In *Proceedings of the IEEE/ACIS 23rd international conference on software engineering, artificial intelligence, networking and parallel/distributed computing* (pp. 162-167). Taichung: IEEE. doi: 10.1109/SNPD54884.2022.10051799.
[22] Leal, O.J.U, Fekete, A., Eudave, R.R., Matos, J.C., Sousa, H., & Teixeira, E.R. (2024). A systematic review of integrated frameworks for resilience and sustainability assessments for critical infrastructures. *Structural Engineering International*, 34(2), 266-280. doi: 10.1080/10168664.2023.2265965.
[23] Li, J., Benaben, F., Gou, J., & Mu, W. (2025). Modeling cascading effects in collaborative systems: A formal risk interdependency framework. *Journal of Modelling in Management*, 20(5), 1711-1737. doi: 10.1108/JM2-09-2024-0313.
[24] Liu, T., & Liu, F. (2025). Graph neural networks for evaluating the reliability and resilience of infrastructure systems: A systematic review of models, applications and future directions. *IEEE Access*, 13, 164883-164904. doi: 10.1109/ACCESS.2025.3611333.
[25] Nguyen, H.X., Zhu, S., & Liu, M. (2022). A survey on graph neural networks for microservice-based cloud applications. *Sensors*, 22(23), article number 9492. doi: 10.3390/s22239492.
[26] Peralta, A., Olivas, J.A., Navarro-Illana, P., & Alvarado, J. (2025). A hybrid mathematical framework for dynamic incident prioritization using fuzzy Q-learning and text analytics. *Mathematics*, 13(12), article number 1941. doi: 10.3390/math13121941.
[27] Pevnev, V.I. (2026). *Methods for optimising an integrated video surveillance system incorporating data analysis*. (PhD dissertation, National Aviation University, Kyiv, Ukraine).
[28] Raptaki, M., Stergiopoulos, G., & Gritzalis, D. (2024). Automated event log analysis with causal dependency graphs for impact assessment of business processes. *IEEE Access*, 12, 194322-194339. doi: 10.1109/ACCESS.2024.3520420.
[29] Reyes-Acosta, R.E., Mendoza-González, R., Oswaldo Diaz, E., Vargas Martin, M., Luna Rosas, F.J., Martínez Romo, J.C., & Mendoza-González, A. (2025). Cybersecurity conceptual framework applied to edge computing and internet of things environments. *Electronics*, 14(11), article number 2109. doi: 10.3390/electronics14112109.
[30] Rötzer, S., Schweigert-Recksiek, S., Thoma, D., & Zimmermann, M. (2022). Attribute dependency graphs: Modelling cause and effect in systems design. *Design Science*, 8, article number e27. doi: 10.1017/dsj.2022.20.
[31] Samia, D., & Innal, F. (2023). An extension of the failure mode effects and criticality analysis with fuzzy analytical hierarchy process method to assess the emergency safety barriers. *International Journal of Industrial Engineering: Theory, Applications and Practice*, 30(2), 474-490. doi: 10.23055/ijietap.2023.30.2.8519.
[32] Šarūnienė, I., Martišauskas, L., Krikštolaitis, R., Augutis, J., & Setola, R. (2024). Risk assessment of critical infrastructures: A methodology based on criticality of infrastructure elements. *Reliability Engineering & System Safety*, 243, article number 109797. doi: 10.1016/j.ress.2023.109797.
[33] Savchenko, T., Vlasenko, L., & Pilat, M. (2025). Analysis of cyberattack dynamics and penetration testing processes using a multilayer risk model and graph-based structures. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique"*, 3(31), 679-697. doi: 10.28925/2663-4023.2025.31.1056.
[34] Schweikert, A.E., L'Her, G.F., & Deinert, M.R. (2021). Simple method for identifying interdependencies in service delivery in critical infrastructure networks. *Applied Network Science*, 6, article number 44. doi: 10.1007/s41109-021-00385-4.
[35] Sperstad, I.B., Solvang, E.H., & Jakobsen, S.H. (2021). A graph-based modelling framework for vulnerability analysis of critical sequences of events in power systems. *International Journal of Electrical Power & Energy Systems*, 125, article number 106408. doi: 10.1016/j.ijepes.2020.106408.
[36] Wen, C. (2024). Modeling evolving service dependencies: Dynamic graph learning for microservice anomaly detection. *Artificial Intelligence and Computing Innovations*, 4(3). doi: 10.5281/zenodo.19605186.

[37] Zheng, C., Si, S., Wang, X., Wang, J., Zhang, X., Lv, S., & Sun, L. (2026). A tolerance analysis framework for microservice-based systems against cascading failures. *Cybersecurity*, 9, article number 59. doi: 10.1186/s42400-025-00399-w.
[38] Zhu, L., Fu, X., Liu, X., & Du, S. (2025). Modeling and analysis of cascade failures in Industrial Internet of Things based on task decomposition and service communities. *Computers & Industrial Engineering*, 206, article number 111177. doi: 10.1016/j.cie.2025.111177.

Метод інтегрального оцінювання критичності інцидентів із використанням причинно-наслідкових графів сервісних залежностей

Даніїл Пилипенко
Аспірант
Луцький національний технічний університет
43018, вул. Львівська, 75, м. Луцьк, Україна
https://orcid.org/0009-0004-4404-4715

Анотація. Актуальність дослідження зумовлена необхідністю підвищення точності визначення пріоритетності реагування на події в умовах зростаючої складності цифрових інфраструктур, де взаємозалежність компонентів і каскадне поширення порушень можуть суттєво посилювати масштаби негативних наслідків. Метою дослідження було розроблення підходу до обґрунтованого ранжування інцидентів за рівнем їх критичності з урахуванням взаємозалежності сервісів та масштабу потенційних наслідків. Методологічну основу дослідження становили системний аналіз, абстрагування, формалізація, графове та концептуальне моделювання, застосовані для дослідження сервісних залежностей і обґрунтування підходу до оцінювання критичності інцидентів у складних інформаційних системах. У результаті дослідження встановлено, що традиційні підходи до оцінювання критичності інцидентів є локально орієнтованими та не враховують міжсервісні залежності, каскадні ефекти й архітектурний контекст сучасних сервісно-орієнтованих інформаційних систем, що призводить до недооцінювання системних наслідків. Обґрунтовано, що критичність інциденту формується як інтегральна характеристика, яка залежить не лише від безпосереднього технічного впливу, але й від структурної значущості ураженого сервісу та характеру поширення впливу в мережі залежностей. Показано, що саме поєднання цих факторів забезпечує коректніше відображення реального рівня системного ризику. Запропоновано графову модель сервісної інфраструктури та концептуальний підхід до інтегрального оцінювання критичності, що поєднує технічні, структурні, каскадні та бізнесові показники в межах багаторівневого агрегування. Встановлено, що врахування каскадних ефектів і структурної важливості сервісів є ключовим для точного оцінювання інцидентів, оскільки дозволяє враховувати як прямі, так і непрямі наслідки та визначати потенціал трансформації локальних збоїв у системні порушення. Результати дослідження можуть бути використані фахівцями з кібербезпеки, архітекторами інформаційних систем і аналітиками центрів моніторингу інцидентів у державних та корпоративних IT-інфраструктурах для підвищення точності пріоритизації інцидентів і оцінювання системних ризиків

Ключові слова: цифрова інфраструктура; сервісно-орієнтована архітектура; каскадні ефекти; багатокритеріальний аналіз; інформаційні системи; аналіз ризиків